学校编码：10384　　分类号_____密级_____

学号：X2013230613　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

某医院电子签章系统设计与实现

Design and Implementation of A Hospital Electronic Seal System

吕曼丽

指 导 教 师： 姚 俊 峰 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2015 年 6 月

论文答辩日期： 2015 年 7 月

学位授予日期： 2015 年 9 月

指 导 教 师：_____

答辩委员会主席：_____

2015 年 6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题(组)经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

2015 年　月　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

2015 年　月　日

摘　要

某医院电子签章系统是符合《卫生系统数字证书应用集成规范》，接口符合国家密码管理局、卫生部相关安全认证接口集成规范，能够实现与医院 HIS、LIS、PACS、电子病历、门诊、系统的无缝连接和信息共享的系统。

电子签章系统它可在 WORD、EXCEL、HTML（WEB 页面）、PDF、WPS 文字、FORM 表单、D 图纸、DGN 图纸、XML 数据、TIF 传真文件实现手写电子签名和加盖电子印章；并可将签章和文件绑定在一起，通过密码验证、签名验证、数字证书确保文档防伪造、防篡改、防抵赖，安全可靠。它具有制章的唯一性、不被变造、伪造，签章的真实性，文档完整性、真实性、不可篡改性，验章的真实性、有效性。可信电子签章系统作为可信应用基础平台，为用户日益增加的信息系统（OA 签章、ERP 表单审批签章、业务系统等）提供安全有效签章基础保障。

将“电子签章系统”嵌入到医嘱系统，有效解决医生电子签名，保证电子医嘱的法律效力，保护医患双方的合法权益。数字证书由权威公正的中心签发，通过技术，保证网上信息传送的真实性、完整性、保密性和不可否认性。

关键词：医院；电子签章；数字签名

Abstract

Electronic signature system in a hospital is with the health system of digit al certificates application integration specification ". The interface conforms to t he national cipher Management Bureau, Ministry of health related safety certifi cation interface integration specification, can be achieved with the hospital his, LIS and PACS, electronic medical records, the outpatient service, the system of seamless connection and information sharing system.

Electronic signature software system which can be in the realization of ha ndwritten electronic signature and official seal of the electronic word, Excel, H TML (web page), PDF, WPS text, form, CAD drawings, DGN drawings, XML data, TIF fax file, and signature and file bound together, through the passwor dauthentication, signature verification to ensure the document forgery, tamper pr oof, non repudiation, safe and reliable. It has a chapter only, not to be altered, forged, the authenticity of signatures, the document is complete, authenticity, ta mpering, check chapter of real and effective of. Trusted electronic signature sys tem as a trusted application platform, for increasing user information system (O A signature, signature and stamp of the approval form of ERP, business system, etc.) to provide safe and effective signature based security.

The electronic seal system embedded ordering system, an effective solution to the electronic signature of the doctor, and ensure the effect law of electron ic medical and protect the medical trouble both sides legitimate rights and inte rests.

Key words: Hospital; electronic signature; digital signature

目　录

Contents

第一章 绪 论

1.1 研究目的及意义

本方案旨在根据医院信息管理系统尤其是电子病历系统等医院信息系统对于安全的实际需求，由此探索出相对应的解决医院管理系统安全问题的最佳方案，建立医院的电子签章服务体系，通过证书及其应用相关产品和技术，实现医院业务应用与电子签章服务与有机结合，着眼于服务内容、流程、模式及保障等角度，处理好诸如身份验证、责任认定、授权管理等的医院电子病历系统等系统的安全问题，将电子病历真实性、完整性、有效性等问题妥善处理好，满足医院实际业务需要，建立安全可信的医院医疗业务环境。

在日常工作中，医院往往会生成很多的诸如门诊/住院医生站医嘱、处方、电子病历等文件信息，要求所有文件都由责任医生签名确认，由此形成法律效力。当前我国正全面落实医院信息化管理系统，因此医院分类形成、存档的电子文件数量与日益增，怎样对电子签名技术进行有效的利用，将纸面文件签名彻底代替，确保电子文件拥有相应的法律效力，使得医生与患者两大主体的合法权益都能得到有效的维护，医院管理人员已经集中精力处理这些问题。

本文对在信息化建设中，基于电子签章技术，如何将各种病历、检查检验报告、处方、申请单、护理记录单以及知情同意等所有医疗文书都实现电子化、数字化。如何实现能够规范业务管理、避免医患纠纷、保障最终医疗文件的合法性进行了积极探索。

1.2 国内发展现状

《中华人民共和国电子签名法》于 2005 年正式颁布实施，由此开启了中国电子签章服务迅猛的发展势头，国家也创造了日益完善的政策环境，拥有越来越大的市场规模、数字证书也有着越来越宽的运用范围，初步形成了标准规范机制。

我国的医疗行业经过多年的信息化建设，硬件系统设备已比较完备，随着医院信息化建设日趋成熟，对于信息系统的运用也越来越充分，例如电子病历、LOS、RIS 等等，医院逐渐走上了现代化、信息化、数字化的发展之道，各大医院正在引入或建设适合自身的信息化系统和集成平台，以实现数字化医院的建设。在整个医疗行业的信息化建设进程中，信息化使得工作人员的效率更高，工

作变得更轻松，患者获得了极大的便利，此外医院也因此获得了更好的经济效益。

2005 年 4 月 1 日我国正式施行《中国人民共和国电子签名法》，因此意味着电子签名和手写签名、盖章等形成的法律效力是完全一致的。电子签章技术已经在多个行业中应用，数据电文的流通和保存备案采用可靠的电子签章与手写签名、盖章等形成的法律效力是完全一致的，电子文书（医疗机构）同样是电子业务的一种类别。该法律的颁布实施使得医院机构正在进行的围绕着电子文书档案、电子病历的研发活动创造了非常好的法律环境。

《卫生系统电子签章服务管理办法》由卫生部于 2009 年 12 月 25 日颁发，其中明确：“对于已经建设成功，但是至今仍旧没有对数字证书进行运用的关键卫生信息系统，一定要在尽量短的时间内对数字证书进行运用，从而达到授权管理、身份认证及责任认定等目的”。 《电子病历基本规范（试行）》由卫生部于 2010 年 2 月 22 日颁布实施，其中明确“电子病历一定要使用电子签名的形式。”《江苏省实施〈电子病历基本规范（试行）〉细则》由江苏省卫生厅于 2010 年 5 月 27 日颁布，其中明确“为了保障电子病历在法律上是有效的，要求其使用电子签名这一形式。”

1.3 系统应用前景

21世纪以来，随着计算机应用技术的不断革新，医疗事业信息化建设也不断的深入，各级医疗机构相继建立起自己的医院信息管理系统（即HIS）。因此，传统医疗工作流程和管理手段也发生了相应的改革和创新。

虽然目前医院信息管理系统的建设已较为成熟，但相当一部分医院的医院信息管理系统仍采用“用户名+口令（密码）”的方式登陆；也仍然使用传统手段即在打印出来的文件上手写签名或盖印章确认系统医疗信息的合法性。这样一来，除了使用大量的纸张造成不环保、因签字或盖印章过于繁琐（很多文件需上级医师签字）而增加医务人员的非专业工作负担外这两点缺陷外，更重要的是，因为医患间的关系特殊，加之医院业务也比较典型，这种旧的登陆方式会令系统操作的安全性和不可抵赖性得不到最大保障。

1.4 论文研究内容

有效整合了数字签名技术及电子印章两种技术的应用软件系统，能够在各种电子文档形式中（例如 Word、EXCEL、XML 数据等）达到手写电子签名及

加盖电子印章的目的；还能够绑定文件及签章，借助签名及密码验证、数字正确等形式避免伪造文档、篡改文档、抵赖文档等问题出现。作为可信应用基础平台，可信电子签章系统让使用者越来越多的诸如 ERP 表单审批签章、OA 签章等的信息系统有着更高高效、更加安全的有效签章基础提供切实的保障。

将“电子签章系统”嵌入到医嘱系统，有效解决医生电子签名，确保电子医嘱具有相应的法律效力，让医生与患者两大主体的合法权益得到有效的保证。保证互联网中传递的信息资料是真实完整的、足够保密的、无法抵赖的。

1.5 论文组织结构

本篇论文一共包括六个章节的内容，下面对此文的内容结构进行系统阐述;

第一章为绪论部分，对的医院电子签章系统展开的研究目的、研究内容进行了详细的阐述，并进一步介绍如今此技术在世界范围内的发展状况及研究焦点，对的医院电子签章系统应用前景进行分析；

第二章主要阐述了基本概念和有关技术分析内容，例如关键的 PKI 和数字签名与验签技术等，为后期方案制定与系统设计打下基础；

第三章 系统需求分析，对基于的医院电子签章系统的需求分析，根据医院的实际情况对该系统进行了可行性分析、业务流程分析、用户角色分析、功能性需求分析、非功能性需求分析和安全性分析；

第四章 系统设计，本章分别从系统框架设计、功能性模块设计、数据库设计、安全方案设计四个方面对于系统具体的方案设计进行了阐述。

第五章为系统的实现部分。章首对系统开发工具进行阐述，并且介绍了开发环境与运行环境，接着描述了系统关键模块的关键代码，最后对主要模块的实现进行描述。

第六章为系统测试部分，此章主要目标是将系统测试方案明确，并开展黑盒测试，检测系统功能；

第七章为全文的总结和展望部分，综合概述了系统设计和实现过程，对系统在将来的设计、研发等工作进行了展望。

1.6 本章小结

本章介绍了论文研究的目的和意义，基于数字证书认证中心的电子签章技术在国内的发展现状及应用的前景。并概括了论文的内容和组织结构。

第二章 基本概念及相关技术介绍

2.1 电子签章与电子病历

作为电子签名表现形式之一的电子签名（图 2-1），是通过图像处理技术让转换操作和电子签名盖章文件操作保持完全一致的视觉效果，借助电子签名技术使得电子信息完整性、真实性等得以有效的维护，签名人员因此无法抵赖其责任。

电子签章校验分为身份校验和数字文书校验两部分。身份校验是验证签章者身份是否合法，数字文书校验是指在通过签章服务器对身份以及签章的合法性认证通过后，将签章系统提供的加密机制在电子医疗文书上执行签章的操作，能对所签文书内容进行完整性认证。所签章的电子文书都已经是 CEBX 版式的文件，CEBX 文件具有加密存储功能，可以用来判定和防止文件被篡改。如果对文件进行其他操作（如扫描文件），可以通过是否显示数字水纹，判定文件内容是否被篡改。

图 2-1 电子签章示意图

《中华人民共和国电子签名法》及《电子签章服务管理办法》（信息产业部颁发）于 2005 年 4 月份正式实施，由此使得电子签名在我国的法律效力得以明确。《中华人民共和国电子签名法》第十四条明确：有效的电子签名和手写签名、盖章所拥有的法律效力是一致的。关于电子签名的定义，该法的第十三条也进行了明确，提出：凡是与下面所述相符的电子签名都是有效可靠的：

（一）当将电子签名制作数据应用至电子签名之中，是电子签名人专门享有的权利；

（二）在签署的过程中，电子签名人掌控着电子签名制作数据；

（三）在成功签署之后，可以察觉出对电子签名做出的所有改动；

（四）在成功签署之后，可以察觉出对数据电文所有内容及形式做出的任何改动。

电子病历一定要包含医生签名这一过程，但是能够和电子病历相匹配的只有

电子签名。因此要求电子签名必须具备下面几个条件：首先，在正式发放电子签名之前，一定要对身份进行核实；其次，确保电子签名使用的唯一性，即只有所有者才享用使用电子签名的权力，假若存在其他人也需要使用电子签名的情况，则要求一定要获得电子签名所有者的授权许可，方可生效；三，应该有相应的技术保障保证电子签名本身及它附着的数据电文都不能被随意改动。

2.2 PKI

PKI的英文全称是Public Key Infrastructure，是通过公钥概念与技术等手段来落实、提供安全服务的安全基础设施，有着普适性特征。PKI可以将诸如数字签名、加密等等密码服务和必须具备的证书管理机制、秘钥等提供给全部网络应用。着眼于字面意思去理解，PKI通过公钥理论、公钥技术将能够提供安全服务的基础设施成功构建起来，是当前网络信息安全技术的关键所在。观察下图 2-2能够得知，当前PKI 技术的应用范围和技术十分广泛，例如电子基础设施为人们日常生活提供所需电能，诸如电视、电脑等的电器都属于电子系统的应用。

认证机构是PKI最为关键的执行结构，数字证书使其核心要素。PKI能够将安全服务提供给诸多网络应用，是维护互联网安全的基础设施。

对于所有大规模网络来说，以第三方为基础的信任是一定需要具备的，而且一定是有效的。如果想在诸多人中将第三方信任构建起来，且信任度得以保证，要求必须具备一个权威中心。

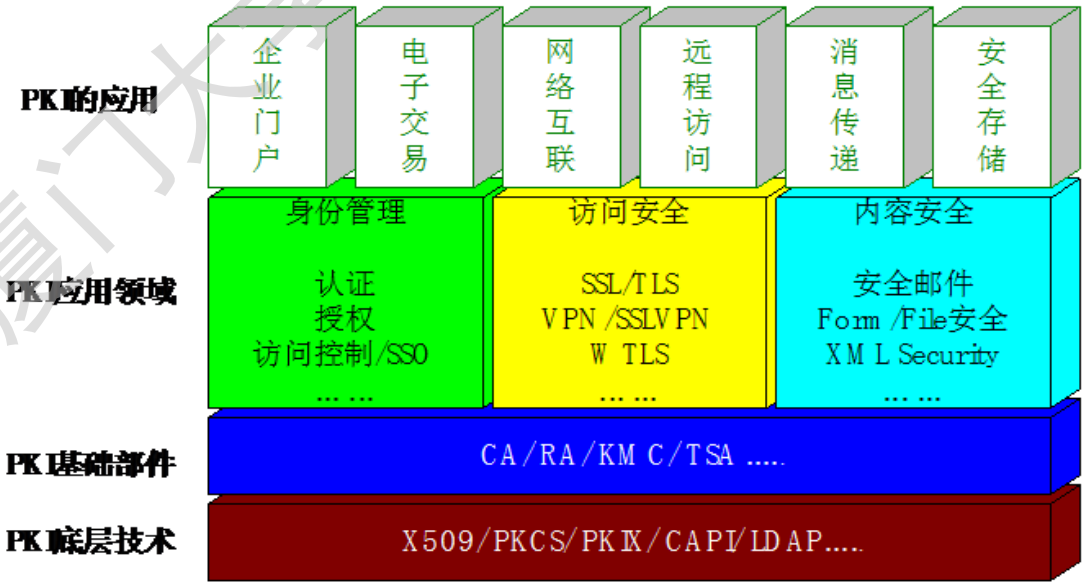

图 2-2 PKI 技术的应用领域与技术

2.3 数字证书

网络通讯过程中，对参与通讯活动的各主体身份信息进行标志的数据即为数据证书，它创造了在互联网中对身份进行验证的方法，也就是在互联网上对诸如“我是谁”“我做了什么”等的问题进行处理，发挥的作用犹如居民身份证。

简而言之数字证书是网络世界中的身份证。在电子文件后附加密钥，能够达到对签名者身份识别、保证签名的不可否认性，同时保证文件内容的真实性和完整性，通过数字证书可以开展数字签名及身份验证活动，持有数字证书的人员如果在互联网中实施了某些操作，将无法抵赖其操作产生的相应责任，除了使操作可靠性得以确保，为将来事件的追踪、责任的明确和纠纷处理提供了有效的根据，

通过散列算法产生摘要，再将非对称秘钥内的私钥调用从而加密摘要产生密文，这一过程即为使用数字证书开展电子签名的原理。

2.4 数字签名与验签

数字签名是通过电子形式在数据信息内存在，或者通过附件形式、逻辑上和它存在关联的数据，能够对数据签署人员的身份进行验证，代表签署人员认可数据信息所涵盖的信息。通过数字签名，可以对下面四个方面的内容进行明确：

1、确保签名人员自主签名发送信息，签名人员无法抵赖；

2、确保在成功签发信息之后直至获取信息没有受到改动，签发文件属于原始文件；

3、将时间戳打在签发的文件内；

4、确保传输时不会泄露文件信息；

非对称加密、报文摘要是实现电子签名技术过程中必须运用到的两种方法，前者常称为 RSA 算法、后者常称为 HASH 算法。签名格式为摘要加公匙，一份签名文件大约增加 2K 签名数据。例如，借助电子印章这一形式来传输电子病历信息，让电子签名及对应病历文件能够融合在一起，授权人之外的人没有权力对此文件进行操作，系统非常可靠，有着较高的安全性。

观察下图 2-4，可知把数字视作证据的最佳手段是对数据开展签名及验签操作。系统借助对用户签名私钥的利用，对数据实施签名运算操作，通过字段的形式于数据库内存储最终的运算结果，在验签数据过程中，系统需要针对用户证书再次开展运算活动，由此签名有效与否就能得以明确。对数据实时签名、验签等